UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND
GREENBELT DIVISION

JEFFREY ERLBAUM
2113 Magnolia Lane
Lafayette Hill, PA 19444,

individually and on behalf of all others similarly situated

Plaintiff,

vs.

MARRIOTT INTERNATIONAL, INC. (a Montgomery County, Maryland Resident)
10400 Fernwood Road
Bethesda, Maryland 20817,

Defendant.

CLASS ACTION

CLASS ACTION COMPLAINT

Jury Trial Demanded

Plaintiff Jeffrey Erlbaum ("Plaintiff"), for himself and all others similarly situated, alleges the following against Defendant Marriott International, Inc. ("Marriott" or "Defendant" or the "Company"), based on personal knowledge as to Plaintiff and Plaintiff's own acts and on information and belief as to all other matters based upon the investigation of Plaintiff's counsel and their review of publicly available information, including news articles, press releases, the Company's website and other publicly available information regarding the Marriott, as to all other matters:

NATURE OF THE ACTION

1. This is a data breach class action brought on behalf of approximately 500 million people whose personal information was exposed due to a flaw in Marriott's guest reservation database systems dating back to 2014, which allowed hackers to take over guests' accounts and access personal information.

2. On November 30, 2018 Marriott announced that there was a data security incident involving the Starwood[1] guest reservation database (the "Marriott Data Breach"). The Marriott Data Breach allowed unauthorized access to guest information relating to reservations at Starwood properties on or before September 10, 2018. The unauthorized party copied and encrypted information from the Starwood guest reservation system and took steps towards removing it. The database contained information on up to approximately 500 million guests who made a reservation at a Starwood property.

3. For approximately 327 million of those guests, the information includes some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guess ("SPG") account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences (collectively, "PII"). Moreover, for some users, the information also includes payment card numbers and payment card expiration dates, although the payment card numbers were encrypted although it is possible that these card numbers were decrypted. For the remaining guests, information accessed was limited to name and sometimes other data such as mailing address, email address or other information.

4. Defendant's conduct—failing to take adequate and reasonable measures to ensure their data systems were protected, failing to take available steps to prevent and stop the breach from ever happening, failing to disclose to Marriott customers the material facts that they did not have adequate computer systems and security practices to safeguard customers' PII, and failing to provide timely and adequate notice of the Marriott Data Breach—has caused substantial consumer harm and injuries to consumers across the United States.

[1] On August 18, 2018, Marriott International and Starwood Hotels & Resorts Worldwide merged, creating the largest hotel company in the world.

5. As a result of the Marriott Data Breach, numerous individuals whose PII were contained in the Starwood guest reservation database have been exposed to fraud and these individuals have been harmed. The injuries suffered by the proposed Class, defined herein, as a direct result of the Marriott Data Breach include:

- theft of their PII;
- costs associated with the detection and prevention of identity theft and unauthorized use of their PII;
- costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the data breach, including purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with all issues resulting from the Marriott Data Breach;
- the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII being placed in the hands of hackers;
- damages to and diminution in value of their PII entrusted to Defendant Marriott for the sole purpose of staying at one of the Company's properties with the mutual understanding that Defendant Marriott would safeguard the PII of Plaintiff and members of the Class against theft and not allow access and misuse of their PII by others; and
- continued risk to their PII, which remains in the possession of Defendant Marriott and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and members of the Class that remains in their possession.

6. Plaintiff seeks to remedy these harms, and prevent their future occurrence, on behalf of himself and all similarly situated individuals whose personal information was comprised as a result of the Marriott Data Breach.

Parties

7. Plaintiff Jeffrey Erlbaum is a resident of Lafayette Hill, Pennsylvania. Erlbaum has stayed at Marriott hotels for decades. On or about November 30, 2018, Plaintiff reviewed news accounts of the Marriott Data Breach.

8. Defendant Marriott, a Delaware corporation, is headquartered at 10400 Fernwood Road, Bethesda, Maryland 20817. Marriott's stock trades on the NASDAQ under the ticker symbol "MAR." Marriott operates, franchises, and licenses hotel, residential and timeshare properties worldwide. The Company operates through three segments: North American Full-Service, North American Limited-Service and Asia Pacific. The Company's properties are operated under the JW Marriott, The Ritz-Carlton, W Hotels, The Luxury Collection, St. Regis, EDITION, Bulgari, Marriott Hotels, Sheraton, Westin, Renaissance, Le Méridien, Autograph Collection, Delta Hotels, Gaylord Hotels, Marriott Executive Apartments, Marriot Vacation Club, Tribute Portfolio, Design Hotels, Courtyard, Residence Inn, Fairfield Inn & Suites, SpringHill Suites, Four Points, TownePlace Suites, Aloft, AC Hotels by Marriott, Protea Hotels, Element and Moxy brand names. As of October 9, 2018, the Company operated approximately 6,700 properties under 30 hotel brand names in 130 countries and territories. Marriott was founded in 1927.

Jurisdiction & Venue

9. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because this a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interests and costs, and

many members of the class are citizens of states different from Defendant. This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

10. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(c) because Defendant is a corporation headquartered in this jurisdiction and regularly transacts business here, and some of the members of the Class reside in this district. Venue is also proper because a substantial part of the events or omissions giving rise to the claims in this action occurred in this District, including decisions by Marriott's management personnel that led to the breach. Moreover, Marriott's terms of service governing its United States members provides for Maryland venue for all claims arising out of Plaintiff's relationship with Marriott.

FACTS

Background

11. Marriott is a worldwide diversified hospitality company that manages and franchises a broad portfolio of hotels and related facilities. It is the largest hotel company in the word, with over 6,500 properties in 127 countries and territories worldwide, accommodating over 1.2 million rooms.

12. To book a stay at one of Marriott's properties, Marriot's guests create, maintain and update profiles containing significant amounts of PII, including their names, birthdates, addresses, email addresses, and payment card information. For international travel, Marriott requires guests to provide their passport number.

13. Marriott collects, stores and maintains PII of its guests including "name, gender, postal address, telephone number, email address, credit and debit card number or other payment data, financial information in limited circumstances…nationality, passport, visa or other government-issued identification data…employer details…geolocation information, social media account ID…." *See* https://www.marriott.com/about/privacy.mi. Marriott collects PII

when a guest "make[s] a reservation, purchases goods and services from [its] Websites or Apps, communicate[s] with [them], or otherwise connect[s] with" Marriott. *Id*.

14. Defendant Marriott recognizes the importance of data privacy and on its website has a section dedicated to privacy. On the Company's website, it states "Marriott International, Inc., Starwood Hotels & Resorts Worldwide, LLC (formerly known as Starwood Hotels & Resorts Worldwide, Inc.) and their affiliates, values you as our guest and recognizes that privacy is important to you." *Id.* Therefore, the Company "seek[s] to use reasonable organizational, technical and administrative measures to protect Personal Data." *Id*.

15. Moreover, the Company's Business Conduct Guide (available at https://www.marriott.com/Multimedia/PDF/CorporateResponsibility/Marriott_Business_Conduct_Guide_English.pdf) has an entire section devoted to "Protecting Confidential Information" (at p. 27-28). The Guide states "Everyone is responsible for protecting the confidentiality of Marriott's proprietary information." Confidential information includes information that might harm Marriott's customers and personal and financial information concerning customers. The policy further states that "Information concerning customers…must be safeguarded." *Id.* at 37.

16. What Defendant failed to tell consumers was that all of these assurances were illusory, as evidenced by the fact that the PII of Plaintiff and members of the Class were exposed to criminals and identity thieves because the Company's systems and controls regarding data security were deficient.

PII Is Valuable

17. The PII compromised in the Marriott Data Breach is extremely valuable to hackers and identity thieves. Names, email address, telephone numbers, payment card information, passport numbers and other valuable PII can be used to gain access to many existing accounts and websites. Hackers and identity thieves use PII to harm Plaintiff and Class

members through blackmail or harassment in person or online, or to commit other types of fraud including obtaining ID cards or driver's licenses, fraudulently obtaining tax returns and refunds and government benefits.

18. Hackers and identity thieves can use PII to harm Plaintiff and Class members through embarrassment, blackmail, and/or harassment in person or online, or to commit other types of fraud including obtaining driver's licenses or identification cards, fraudulently obtaining tax returns and refunds and obtaining government benefits. As a result, individual victims of identity theft can suffer indirect financial costs, including the costs incurred in civil litigation initiated by creditors and in overcoming challenges to obtain and/or retain credit. Victims also need to spend time to repair the damage caused by hackers – time to monitor accounts, check credit reports for inaccuracies and fraudulent charges, close existing financial accounts and reopen new ones and dispute charges with individual creditors.

19. Cyber security firm Trustwave conducted a global study called "The Value of Data." According to Trustwave's vice president of security research, Ziv Mador, "Today, data is one of the most valuable commodities possessed by any business. Whether that data belongs to the organization itself, its employees, suppliers or customers, it has a duty to protect that data to the best of its abilities. Companies that fail to accurately value their data are unlikely to make the right decisions regarding the level of cyber security investments to protect that data and are those most likely to fall short of regulations…"

20. Testimony before the Committee on Financial Services Subcommittee on Terrorism and Illicit Finance before the United States House of Representatives on March 15, 2018 details the value of stolen data and states "cyber black markets offer the computer-hacking tools and services to carry out cybercrime attacks and sell the byproducts stolen in those attacks: credit cards, personal data, and intellectual property." *See T*he Motivations of Cyber Threat

Actors and Their Use and Monetization of Stolen Data Testimony of Lillian Ablon, The RAND Corporation Before the Committee on Financial Services Subcommittee on Terrorism and Illicit Finance United States House of Representatives March 15, 2018 (available at https://financialservices.house.gov/uploadedfiles/hhrg-115-ba01-wstate-lablon-20180315.pdf).

21. The problems associated with identity theft are compounded by the fact that many identity thieves wait years before attempting to use the PII they stole. Indeed, in order to protect himself, Plaintiff will need to remain alert against unauthorized data use for many years to come.

22. Once PII is stolen, it can be used in many ways. Typically, PII is offered for sale on the "dark web", a heavily encrypted part of the Internet that makes it difficult for authorities to detect the location or owners of a website. The dark web exists on an encrypted network and cannot be found by using traditional search engines or visited by using traditional browsers. It is only accessible using a Tor browser or similar tool, which aims to conceal users' identities or online activity. The dark web is known for hosting marketplaces that sell illegal items such as weapons, drugs, and PII.

23. When someone purchases PII, it is used to gain access to different areas of a victim's digital life, including bank accounts, social media, and credit card information. During the process, other sensitive data may be harvested from the victim's accounts, as well as from those belonging to relatives, friends and colleagues.

Marriott's Inadequate Data Security Led to the Marriott Data Breach

24. On November 30, 2018, Defendant Marriott announced an attack on its network that exposed the PII of approximately 500 million users.

25. According to Marriott, it discovered the vulnerability months before on September 8, 2018, "from an internal security tool regarding and attempt to access the Starwood

guest reservation database," and "quickly engaged leading security experts to help determined what occurred." *See* https://answers.kroll.com/.

26. Marriott learned during the investigation that there had been unauthorized access to the Starwood network since 2014. The Company discovered that an unauthorized party had copied and encrypted information, and took steps towards removing it. On November 19, 2018, Marriott was able to decrypt the information and determined that the contents were from the Starwood guest reservation database. *Id.*

27. Of the 500 million guests potentially affected by the Marriott Data Breach, approximately 327 million of the affected guests had information accessed that includes some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest ("SPG") account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences. *Id.* The Marriott website allows states that for "some" of these affected users, the information also includes payment card numbers and payment card expiration dates, but the payment card numbers were encrypted using Advanced Encryption Standard encryption (AES-128). There are two components needed to decrypt the payment card numbers, but Marriott has not been able to rule out the possibility that both were taken. *Id.*

28. For the remaining 173 million guests affected, the information was limited to name and sometimes other data such as mailing address, email address, or "other information" that Marriott has not provided details on, leaving consumers without full knowledge of the extent of the breach of their information.

29. Importantly, while Defendant Marriott was aware of the breach as of September 8, 2018, it waited more than two months to publicly disclose the breach. And those potentially

affected are being notified via on a rolling basis beginning on November 30, 2018, again more than two months after discovery of the breach. *Id*.

30. Marriott did not know the origin or the identity of the hackers. In fact, to date, Marriott has not fully assessed the scope of the attack, despite discovering the attack on September 8, 2018 and engaging "leading security experts." *Id*.

31. Despite numerous data breaches in the hospitality industry and otherwise, Marriott did not employ the best practices and safeguards to protect users' PII and that information remains at risk today and into the future, until Marriott is able to secure the PII stored on hundreds of millions of United States citizens. Indeed, Starwood reported a much smaller breach in 2015, where attackers installed malware on point-of-sale systems in some hotel restaurants and gift shops to siphon off payment card information. *See* McMillan, Robert, "Marriott's Starwood Missed Chance to Detect Huge Data Breach Years Earlier, Cybersecurity Specialists Say; Attack in 2015 Could Have Prompted Hotel Operator to Investigate and Find Hackers who Lurked in its Computer System, Experts Say," *The Wall Street Journal*, December 2, 2018. It disclosed this attack four days after Marriott announced a deal to acquire Starwood. Although Marriott is saying that the 2015 is different and not related to the Marriott Data Breach, security specialists say a more thorough investigation into the 2015 attack could have uncovered the attackers, who instead were able to lurk in the reservation systems for three more years. *Id*.

32. The Marriott Data Breach has also attracted the attention of Attorneys General from at least five states and likely several more in the near future. Specifically, on November 30, 2018, Maryland Attorney General Brian Frosh announced that he was "launching an investigation into a massive data security breach affecting as many as 500 million guests who stayed at hotels operated by Marriott Corp." Frosh called the Marriott Data Breach "one of the

largest and most alarming we've seen." *See* https://www.baltimoresun.com/news/maryland/politics/bs-md-frosh-marriott-20181130-story.html. Likewise, the Attorneys General of Illinois, New York, Texas and Massachusetts have announced that they were investigating the Marriott Data Breach. The Federal Bureau of Investigation also said it is tracking the Marriott Data Breach.

Marriott Failed to Comply with FTC Regulations

33. Federal and state governments have established security standards and issued recommendations to prevent data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses highlighting the need for data security practices. The FTC has stated that the need for data security should be factored into all business decision-making. *See* Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-langage/pdf0205-starwithsecurity.pdf.

34. The FTC updated its publication *Protecting Personal Information: A Guide for Business*, in 2016. That publication established guidelines for fundamental data security principles and practices for business. The guideline notes businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information that is stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The FTC guide also recommends that businesses use an intrusion detection system to expose a breach as soon as it happens; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a data breach.

35. Further, the FTC recommends that businesses only store information for as long as is needed for authorization of a transaction; limit access to sensitive data; require complex passwords be used on networks, use industry-tested methods for security; monitor for suspicious activity on the network and verify that third-party service providers have implemented appropriate security measures. *See* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

36. The FTC has brought enforcement actions against businesses that fail to adequately and reasonably protect customer data, treating such failure as a unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (the "FTCA"), 15 U.S.C. § 45.

37. Here, Marriott was, or should have been, fully aware of its obligation to protect the PII of its guests and customers. Marriott was, or should have been, aware of the significant repercussions if it failed to do so because it collected the payment card date from hundreds of millions of guests and customers daily and they knew if this data was hacked, it would result in injury to consumers, including Plaintiff and the Class.

38. Nevertheless, Marriott failed to take appropriate protective and preventive measures to secure guests' PII, including that of Plaintiff and the Class.

39. Despite understanding the consequences of inadequate data security, Marriott operated its computer guest reservations system without outdated operating systems and software; failed to enable point-to-point and end-to-end encryption; failed to detect intrusions dating as far back as 2014; and failed to take other necessary measures to protect the security of its network.

The Harm Caused by the Marriott Data Breach

40. Without timely and detailed disclosure to its guests and customers, consumers, including Plaintiff and Class members, were unknowingly left exposed to continued misuse and

ongoing risk of misuse of their PII for months and even years and were therefore unable to take necessary precautions to prevent imminent harm.

41. The consequences of the Marriott Data Breach are severe. PII is valuable to hackers and identity thieves and once the information has been compromised, identity thieves "can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance." *See* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft. The information Marriott failed to keep secure can be used by hackers to perpetrate a variety of crimes that harm victims including: immigration fraud, obtaining a driver's license or identification card in the victim's name, or filing fraudulent tax returns.

42. A 2016 survey found that the "quicker a financial institution, credit card issuer…or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit damage. Early notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act." *See* https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new.

43. Marriott's almost three-month delay in notifying consumers of the Marriott Data Breach therefore increased the risk of fraud for Plaintiff and the Class members.

44. A consumer whose identity has been stolen cannot be made whole from monetary reimbursement. Rather, identity theft victims must spend countless hours to repair the impact to their credit and to resolve the other consequences of such fraud.

45. Also, there is frequently a lag time between when the harm occurs (data is stolen) and when it is used. Thus, Plaintiff and the Class now face years of constant monitoring and surveillance of their financial accounts and personal records. Plaintiff and the Class are

incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them and the resulting loss of use of their credit and access to funds, regardless of whether such charges are ultimately reimbursed by financial institutions.

Plaintiff and Class Members Suffered Damages as a Result of the Marriott Data Breach

46. As described herein, PII is private and sensitive and was left inadequately protected by Marriott. Marriott never obtained the consent of Plaintiff and the Class members to disclose their PII to any other person as required by law and applicable industry standards.

47. The Marriott Data Breach was a direct and proximate result of the Company's failure to properly safeguard and protect the PII of Plaintiff and the members of the Class from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Marriott's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and the Class members PII to protect against reasonably foreseeable threats to the integrity of such information.

48. Marriott had the resources to prevent such a breach, but neglected to adequately invest in data security, despite the growing number of data breaches and a 2015 attack to the Starwood system.

49. Had Marriot remedied the deficiencies and vulnerabilities in its information storage and security systems, followed industry guidelines and best practices, and adopted security measures recommended by experts, the Marriott Data Breach and theft of Plaintiff's PII could have been prevented.

50. As a direct and proximate result of Marriott's wrongful actions and inaction and the resulting Marriott Data Breach, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity

fraud, requiring them to take the time which they otherwise would have dedicated to other life demands in an effort to mitigate the actual and potential impact of the Marriott Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured.

51. As detailed *supra*, Marriott's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation.

52. Marriott continues to hold consumers' PII, including Plaintiff and Class members. Because Marriott has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiff and Class members have an undeniable interest in ensuring that their PII is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

Marriott's Offer to Monitor Credit of Consumers is Inadequate

53. As announced on the website detailing the Marriott Data Breach, the Company has offered one year of free enrollment in "WebWatcher," which monitors internet sites where PII is shared and generates alerts if evidence of the consumer's PII is found.

54. As detailed herein, consumers' PII may exist on the dark web for months, or even years, before it is used for ill gains and actions. With only one year of monitoring, and no form of insurance or other protection, Plaintiff and Class members remain unprotected from the real and long-term threats against their PII. Therefore, the "monitoring" services offered by

Marriott are inadequate, and Plaintiff and Class Members have a real and cognizable interest in obtaining equitable relief, in addition to the monetary relief requested herein.

CLASS ACTION ALLEGATIONS

55. Plaintiff brings all of his claims as class claims under Federal Rule of Civil Procedure 23. The requirements of Federal Rule of Civil Procedure 23(b)(2), 23(b)(3) and 23(c)(4) are met with respect to the Class defined below.

56. The Plaintiff Class consists of:

> All persons in the United States who provided personal information to Marriott and whose personal information was accessed, compromised or stolen by unauthorized individuals in the data breach announced by Marriott on November 30, 2018.

57. Excluded from the Class is Defendant and any entities in which any Defendant or its subsidiaries or affiliates have a controlling interest, and Defendant's officers, agents, and employees. Also excluded from the Class is the judge assigned to this action, members of the judge's staff, and any member of the judge's immediate family.

58. The Class is so numerous that joinder of all members is impracticable. The Class includes approximately 500 million individuals whose personal information was compromised by the Marriot Data Breach. The names and addresses of Class members are identifiable through documents maintained by Marriott.

59. There are numerous questions of law and fact common to Plaintiff and the Class, including the following:

- whether Defendants engaged in the wrongful conduct alleged herein;
- whether Class members' PII was accessed, compromised, or stolen in the Marriott Data Breach;

- whether Defendants owed a duty to Plaintiff and members of the Class to adequately protect their PII and to provide timely and accurate notice of the Marriott Data Breach to Plaintiff and members of the Class;
- whether Defendant breached its duties to protect the PII of Plaintiff and members of the Class by failing to provide adequate data security and whether Defendant breached its duty to provide timely and accurate notice to Plaintiff and members of the Class;
- whether Defendants knew or should have known that their computer systems were vulnerable to attack;
- whether Defendant unlawfully failed to inform Plaintiff and members of the Class that it did not maintain computers and security practices adequate to reasonably safeguard PII and whether Defendant failed to inform Plaintiff and members of the Class of the data breach in a timely and accurate manner;
- whether Plaintiff and members of the Class suffered injury, including ascertainable losses, as a result of Defendants' conduct (or failure to act);
- whether Defendant knew about the Data Breach before it was announced to the public and Defendant failed to timely notify the public of the Marriott Data Breach;
- Whether Defendant's conduct violated § 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, *et seq.*;
- whether Plaintiff and members of the Class are entitled to recover damages; and
- whether Plaintiff and Class members are entitled to equitable relief, including injunctive relief and/or other equitable relief.

60. Plaintiff's claims are typical of the claims of the Class in that the representative Plaintiff, like all Class members, had his personal information compromised in the Marriott Data Breach.

61. Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has retained counsel who is experienced in class-action and complex litigation. Plaintiff has no interests that are adverse to, or in conflict with, other members of the Class.

62. The questions of law and fact common to the Class members predominate over any questions which may affect only individual members.

63. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class members would likely find the cost of litigating their claims prohibitively high and would therefore have no effective remedy.

64. The prosecution of separate actions by the individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

65. Defendant has acted on grounds that apply generally to the Class so that injunctive relief under Fed. R. Civ. P. 23(b)(2) is appropriate with respect to the Class as a whole.

CLAIMS

COUNT I – NEGLIGENCE

66. Plaintiff incorporates by reference those paragraphs set out above as if fully set forth herein.

67. Defendant Marriott owed a duty to Plaintiff and the Class to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in their

possession from being compromised, stolen, lost, accessed, misused and/or disclosed to unauthorized recipients. This duty included, among other things, designing, maintaining, and testing Defendant's security systems to ensure the PII of Plaintiff and the Class was adequately secured and protected, including using encryption software and technologies. Defendant also had the duty to implement processes that would detect a breach of its security in a timely manner and to timely act upon warnings and alerts.

68. Defendants owed a duty to timely disclose the material fact that their computer systems and data security practices were inadequate to safeguard individuals' PII.

69. Defendant breached these duties by the conduct alleged in the Complaint by, including without limitation, (a) failing to protect the PII; (b) failing to maintain adequate computer systems and data security practices to safeguard the PII; (c) failing to disclose the material fact that Defendant's computer systems and data security practices were inadequate to safeguard the PII; and (d) failing to disclose in a timely and accurate manner to Plaintiff and members of the Class the material fact of the Marriott Data Breach.

70. The conduct alleged herein caused Plaintiff and Class members to be exposed to fraud and be harmed as detailed herein.

71. Plaintiff and Class members were foreseeable victims of Defendant's inadequate data security practices and in fact suffered damages caused by Defendant's breaches of their duties.

72. Defendant Marriott knew the PII of Plaintiff and the Class was personal and sensitive information, which is valuable to identity thieves and cyber criminals. Defendant also knew of the serious harms that could result through the wrongful disclosure of the PII of Plaintiff and the Class.

73. Because Plaintiff and the Class entrusted Defendant Marriott with their PII, Defendant had a special relationship with Plaintiff and the Class. Plaintiff and the Class signed up and paid for Defendant's hospitality services and agreed to provide their PII with the understanding that Defendant would take appropriate measures to safeguard it, and would timely inform Plaintiff and the Class of any breaches or other security concerns that might call for action by Plaintiff and the Class. As alleged herein, Defendant did not. Defendant is morally culpable, given the prominence of security breaches today, especially in the hospitality industry and especially given the admission that this data vulnerability dates back to 2014. This demonstrates that Defendant's had inadequate safeguards to protect Plaintiff and the Class from breaches or security vulnerabilities.

74. Defendant's failure to comply with industry standards and federal regulations further demonstrates its negligence in failing to exercise reasonable care in safeguarding and protecting the PII of Plaintiff and the Class.

75. Defendant's breaches of these duties were not isolated incidents or small mistakes. The breaches set forth herein resulted from long-term Company-wide refusal to acknowledge and correct serious ongoing data security problems dating back to at least 2014.

76. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and the Class, their PII would not have been compromised, stolen and accessed by unauthorized persons. Defendant's negligence was a direct and legal cause of the theft of Plaintiff's and the Class's PII and all resulting damages

77. The injury and harm suffered by Plaintiff and the Class was a reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting the PII of Plaintiff and the other Class members. Defendant knew its guest

reservation systems and technologies for processing and securing PII had numerous security vulnerabilities.

78. As a result of Defendant's misconduct, the PII of Plaintiff and the Class was compromised, placing them at a greater risk of identity theft and their PII was disclosed to third parties without their consent. Plaintiff and Class members also suffered diminution in the value of their PII in that it is now easily accessible to hackers on the Dark Web. Plaintiff and the Class have also suffered out of pocket losses form procuring credit protection services, identity theft monitoring and other expenses related to identity theft losses or protective measures.

79. Defendant's misconduct alleged herein is malice or oppression, in that it was carried out with a willful and conscious disregard of the rights or safety of Plaintiff and the Class and conduct that subjected Plaintiff and the Class to unjust hardship in conscious disregard of their rights.

COUNT II – NEGLIGENCE *PER SE*

80. Plaintiff incorporates by reference those paragraphs set out above as if fully set forth herein.

81. Section 5 of the FTC Act prohibits "unfair…practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Marriott, of failing to use reasonable measures to protect PII. The FTC publications and orders described *supra* also form part of the basis for Marriott's duty in this regard.

82. Marriott violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described herein. Marriott's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored – approximately 500 million unique guests and consumers – and the foreseeable

consequences of a data breach at a hospitality chain as large as Marriott, including, specifically, the immense damages that would result to Plaintiff and the Class.

83. Marriott's violation of Section 5 of the FTC Act constitutes negligence *per se*.

84. Plaintiff and the Class are within the class of persons that the FTC Act was intended to cover.

85. The hard that occurred as a result of the Marriott Data Breach is the type of harm that the FTC Act was intended to protect against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable safeguards to ensure data security and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

86. As a direct and proximate result of the Company's negligence *per se*, Plaintiff and the Class have suffered, and will continue to suffer, injuries and damages arising from identity theft; Plaintiff's inability to use their debit or credit cards because those cards were cancelled, suspended or otherwise rendered unusable as a result of the Marriott Data Breach and/or false or fraudulent charges stemming from the Marriott Data Breach, including but not limited to late fees charged and foregone cash back rewards; damages from lost time to mitigate the actual and potential impact of the Marriott Data Breach on their lives, including, among other things, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring credit reports and accounts for unauthorized access and activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

87. Moreover, as a direct and proximate result of the Company's negligence *per se*, Plaintiff and Class members have suffered and will continue to suffer the risks of exposure of

their PII, which remain in Marriott's possession and is subject to further unauthorized disclosures so long as Marriott fails to undertake appropriate and adequate measures to safeguard the PII in its possession.

COUNT III – BREACH OF CONFIDENCE

88. Plaintiff incorporates by reference those paragraphs set out above as if fully set forth herein.

89. At all times during Plaintiff and the Class members' interactions with Marriott, Marriott was fully aware of the confidential and sensitive nature of the PII that Plaintiff and the Class members provided to Marriott.

90. As alleged herein, Marriott's relationship with Plaintiff and the members of the Class was governed by expectations that their PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

91. Plaintiff and Class members provided their PII to Marriott with the explicit and implicit understanding that Defendant would protect and not allow the PII to be accessed by or disseminated to any unauthorized parties.

92. Plaintiff and Class members also provided their respective PII to Defendant with the explicit and implicit understanding that Defendant would take precautions to protect that PII from unauthorized disclosure, such as following the basic principles of information security practices.

93. Defendant voluntarily received in confidence the PII of Plaintiff and the Class with the understanding that it would not be disclosed or disseminated to the public or any unauthorized parties.

94. Because of Defendant's failure to prevent, detect, and/or avoid the Marriott Data Breach from occurring by, *inter alia*, failing to follow best information security practices to

secure the PII of Plaintiff and the Class, Plaintiff's and the Class members' Customer Data was disclosed and misappropriated to unauthorized third parties without their express permission.

95. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and the Class have suffered damages as alleged herein.

96. But for Defendant's disclosure of Plaintiff's and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed and used by unauthorized third parties. The Marriott Data Breach was the direct and legal cause of the theft of the PII of Plaintiff and the Class, as well as of the resulting damages.

97. The injury and harm alleged herein was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' PII. Defendant knew that its systems had numerous security vulnerabilities because Defendant failed to follow industry standard information security practices, including Marriott's inability to detect the Marriott Data Breach as far back as 2014.

98. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Class have suffered, and will continue to suffer, injuries and damages resulting from identity theft; Plaintiff's inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Marriot Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charged and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives, including, among other things, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing or monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages

from identity theft, which may take months or years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

99. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT IV – VIOLATION OF MARYLAN'S CONSUMER PROTECTION ACT, MARYLAND CODE ANN., COM. LAW § 13-101 *et seq.*

100. Plaintiff incorporates by reference those paragraphs set out above as if fully set forth herein.

101. This count is brought under the Maryland Consumer Protection Act, Md. Code Ann. Com. Law ("CL") § 13-101 *et seq.*

102. Plaintiff is a consumer for the purposes of Maryland's Consumer Protection Act.

103. Defendant is a merchant for the purposes of Maryland's Consumer Protection Act. Marriott, was at all relevant times, engaged in soliciting "consumer services" as that term is defined by CL § 13-101(d) by soliciting an ongoing service, credit reporting and data aggregation of Plaintiff's personal information, to consumers in Maryland for primarily personal use within the meanings of the Act.

104. Marriott is also a "person" as that term is defined in CL § 13-101(h), as Marriott was, at all relevant times, a legal or commercial entity.

105. By failing to inform consumers, including Plaintiff and the Class members, of Defendant's unsecure, uncompliant, and otherwise insufficient data and information security practices, Defendant advertised, sold, serviced, and otherwise induced those consumers to purchase goods and services from Defendant.

106. Defendant, by failing to inform consumers (including Plaintiff and the Class members) of its unsecure, uncompliant, and other insufficient data and information security practices, falsely represented the security of their data and information security practices to safeguard the consumer's PII Defendant collected.

107. Maryland law also requires notification of data breaches upon identification. Defendant identified the Marriott Data Breach as early as September 2018, but only notified consumers nearly three months later on November 30, 2018, thus placing those consumers at additional risk for the months in between the discovery and notification of the Marriott Data Breach.

108. Defendant's failures constitute false, misleading misrepresentations concerning the security of the networks and aggregation of PII. These misrepresentations could and did deceive and/or mislead consumers concerning the safety of their PII.

109. In addition, the facts upon which consumers (including Plaintiff and the Class) relied were material facts, the veracity of which were not true (i.e., protection of PII), and consumers relied on those false facts to their detriment.

110. Defendant employed these false representations to promote the sale of a consumer good or service, which Plaintiff and the Class purchased.

111. As a direct and proximate results of the breaches of confidence alleged herein, Plaintiff and the Class have suffered, and will continue to suffer, other forms of injury and/or harm, including but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, respectfully request that the Court enter judgment against Defendants, as follows:

1. Certifying the Class, and appointing Plaintiff as Class Representative;

2. Finding Defendant Marriott's conduct was negligent, deceptive, unfair and unlawful as alleged herein;

3. Injunctive relief requiring Defendant to implement measures that strengthen its data security protocols and provide for periodic audits of those protocols and preventing Defendant from engaging in further negligent, deceptive, unfair and unlawful business practices;

4. An award to Plaintiff and the Class members of actual, compensatory, and consequential damages;

5. An award to Plaintiff and the Class members of statutory damages and penalties, as allowed by law;

6. An award to Plaintiff and the Class members of restitution and disgorgement;

7. An award to Plaintiff and the Class members of punitive damages;

8. Requiring Defendant to take appropriate measures to remediate the damage caused to Plaintiff and the Class;

9. An award of attorneys' fees, costs, and expenses, as provided by law, or equity, or as otherwise available;

10. An award of pre-judgment and post-judgment interest, as provided by law or equity; and

11. Such other or further relief as may be appropriate under the circumstances.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of any and all issues in this action so triable of right.

Dated: December 6, 2018

Respectfully submitted,

/s/ Hassan Zavareei
Hassan Zavareei (No. 18489)
TYCKO & ZAVAREEI LLP
1828 L. Street, NW, Suite 1000
Washington, DC 20036
hzavareei@tzlegal.com
Tel: (202) 973-0910
Fax: (202) 973-0950

Jeffrey W. Golan
Stephen R. Basser
Julie B. Palley
BARRACK, RODOS & BACINE
3300 Two Commerce Square
2001 Market Street
Philadelphia, Pennsylvania 19103
Telephone: (215) 963-0600
Facsimile: (215) 963-0838
jgolan@barrack.com
sbasser@barrack.com
jpalley@barrack.com

Attorneys for Plaintiff